

BUDGET LETTER

SUBJECT: SAFEGUARDING ACCESS TO STATE DATA	NUMBER: 04-35
REFERENCES: STATE ADMINISTRATIVE MANUAL SECTIONS 4840.4, 4841.2 4841.3	DATE ISSUED: November 16, 2004
	SUPERSEDES:

TO: Agency Secretaries
Department Directors
Departmental Budget Officers
Departmental Chief Information Officers
Departmental Information Security Officers
Department of Finance Budget Staff

FROM: DEPARTMENT OF FINANCE

Note: Budget Officers are requested to forward a copy of this Budget Letter (BL) to your department's Information Security Officers (ISOs) and department's Chief Information Officers (CIOs). The Finance State ISO Office will also distribute this BL separately to the ISOs and CIOs on the current contact list.

BACKGROUND

The Department of Finance (Finance) is responsible for establishing the framework for the State's information technology (IT) security policies and activities, and for IT security oversight. This BL expands upon and clarifies policy about protecting the State's information resources.

The State Administrative Manual (SAM) Section 4841.2, Information Integrity and Security, requires that each agency provide for the integrity and security of its automated files and databases. New policy in this section requires written agreements with vendors, consultants, or researchers before they are allowed access to State data.

Although some agencies already have practices in place that support these policies, it is critical that State data in all agencies be protected through good policy and practice.

POLICY

The following definition and policy are effective immediately. The changes will appear in the next update of the SAM. You may refer to Attachment I, "Advance Copy of Changes to State Administrative Manual Sections 4840.4 and 4841.2," to see the context of this policy change.

Definition:

Non-State Entity. A business, organization, or individual that is not a State entity, but requires access to State information assets in conducting business with the State. (This definition includes, but is not limited to, researchers, vendors, consultants, and their employees, and entities associated with federal and local government and other states.)

Policy:

Each agency must provide for the integrity and security of its information assets by ensuring that responsibility for each automated file or database is defined.

Every agency must establish appropriate policies and procedures for preserving the integrity and security of each automated file or database. This requirement includes the use of agreements with non-state entities, to cover, at a minimum, the following:

- Appropriate levels of confidentiality for the data, based on data classification (see SAM section 4841.3);
- Standards for transmission and storage of the data, if applicable;
- Agreement to comply with all State policy and law regarding use of information resources and data;
- Signed confidentiality statements;
- Agreement to apply security patches and upgrades, and keep virus software up-to-date on all systems on which the data may be used; and
- Agreement to notify the State data owners promptly if a security incident involving the data occurs.

CONTACTS AND QUESTIONS

You may call the State ISO Office at (916) 445-5239 if you have questions about this BL or about the practices.

/s/ Veronica Chung-Ng

Veronica Chung-Ng
Program Budget Manager

Attachment

Advance Copy of Changes to State Administrative Manual Sections 4840.4 and 4841.2

New text is in italics; nothing was deleted.

4840.4 DEFINITIONS

Confidential Information. Information maintained by state agencies that is exempt from disclosure under the provisions of the California Public Records Act (Government Code Sections 6250-6265) or other applicable state or federal laws. See SAM Section 4841.3.

Critical Application. An application that is so important to the agency that its loss or unavailability is unacceptable. With a critical application, even short-term unavailability of the information provided by the application would have a significant negative impact on the health and safety of the public or state workers; on the fiscal or legal integrity of state operations; or on the continuation of essential agency programs.

Custodian of Information. An employee or organizational unit (such as a data center or information processing facility) acting as a caretaker or an automated file or database.

Disaster. A condition in which an information asset is unavailable, as a result of a natural or man-made occurrence, that is of sufficient duration to cause significant disruption in the accomplishment of agency program objectives, as determined by agency management.

Hardening. A defense strategy to protect against attacks by removing vulnerable and unnecessary services, patching security holes, and securing access controls.

Information Assets. (1) All categories of automated information, including (but not limited to) records, files, and databases; and (2) information technology facilities, equipment (including personal computer systems), and software owned or leased by state agencies.

Information Integrity. The conditions in which information or programs are preserved for their intended purpose; including the accuracy and completeness of information systems and the data maintained within those systems.

Information Security. The protection of automated information from unauthorized access (accidental or intentional), modification, destruction, or disclosure.

Owner of Information. An organizational unit having responsibility for making classification and control decisions regarding an automated file or database.

Non-State Entity. *A business, organization, or individual that is not a State entity, but requires access to State information assets in conducting business with the State. (This definition includes, but is not limited to, researchers, vendors, consultants, and their employees, and entities associated with federal and local government and other states.)*

Physical Security. The protection of information processing equipment from damage, destruction or theft; information processing facilities from damage, destruction or unauthorized entry; and personnel from potentially harmful situations.

Advance Copy of Changes to State Administrative Manual Sections 4840.4 and 4841.2

Privacy. The right of individuals and organizations to control the collection, storage, and dissemination of information about themselves.

Public Information. Any information prepared, owned, used, or retained by a state agency and not specifically exempt from the disclosure requirements of the California Public Records Act (Government Code Sections 6250-6265) or other applicable state or federal laws.

Risk. The likelihood or probability that a loss of information assets or breach of security will occur.

Risk Analysis. The process of evaluating: (a) the vulnerability of information assets to various threats, (b) the costs or impact of potential losses, and (c) the alternative means of removing or limiting risks.

Risk Management. The process of taking actions to avoid risk or reduce risk to acceptable levels.

Sensitive Information. Information maintained by state agencies that requires special precautions to protect it from unauthorized modification, or deletion. See SAM Section 4841.3. Sensitive information may be either public or confidential (as defined above).

User of Information. An individual having specific limited authority from the owner of information to view, change, add to, disseminate or delete such information.

4841.2 INFORMATION INTEGRITY AND SECURITY

Each agency must provide for the integrity and security of its information assets by:

1. Identifying all automated files and databases for which the agency has ownership responsibility (see SAM Section 4841.4);
2. Ensuring that responsibility for each automated file or database is defined with respect to:
 - a. The designated owner of the information within the agency;
 - b. Custodians of information; and
 - c. Users of the information;
 - d. Ensuring that each automated file or database is identified as to its information class (SAM Section 4841.3) in accordance with law and administrative policy;
 - e. Establishing appropriate policies and procedures for preserving the integrity and security of each automated file or database including:
 1. *Agreements with non-state entities to cover, at a minimum, the following:*

Advance Copy of Changes to State Administrative Manual Sections 4840.4 and 4841.2

- a. Appropriate levels of confidentiality for the data based on data classification (see SAM Section 4841.3);*
 - b. Standards for transmission and storage of the data, if applicable;*
 - c. Agreement to comply with all State policy and law regarding use of information resources and data;*
 - d. Signed confidentiality statements;*
 - e. Agreement to apply security patches and upgrades, and keep virus software up-to-date on all systems on which data may be used; and*
 - f. Agreement to notify the State data owners promptly if a security incident involving the data occurs.*
 2. Identifying computing systems that allow dial-up communication or Internet access to sensitive or confidential information and information necessary for the support of agency critical applications;
 3. Auditing usage of dial-up communications and Internet access for security violations;
 4. Periodically changing dial-up access telephone numbers; and
 5. Responding to losses, misuse, or improper dissemination of information.
3. Establishing appropriate departmental policies and procedures to protect and secure IT infrastructure, including:
 - a. Technology upgrade policy, which includes, but is not limited to, operating system upgrades on servers, routers, and firewalls. The policy must address appropriate planning and testing of upgrades, in addition to departmental criteria for deciding which upgrades to apply.
 - b. Security patches and security upgrade policy, which includes, but is not limited to, servers, routers, and firewalls. The policy must address application and testing of the patches and/or security upgrades, in addition to departmental criteria for deciding which patches and security upgrades must be applied, and how quickly.
 - c. Firewall configuration policy, which must require creation and documentation of a baseline configuration for each firewall, updates of the documentation for all authorized changes, and periodic verification of the configuration to ensure that it has not changed during software modifications or rebooting of the equipment.
 - d. Server configuration policy, which must clearly address all servers that have any interaction with Internet, extranet, or intranet traffic. The policy must require creation and documentation of a baseline configuration for each server, updates of the documentation for all authorized changes, and periodic checking of the configuration to ensure that it has not changed during software modifications or rebooting of the equipment.

Advance Copy of Changes to State Administrative Manual Sections 4840.4 and 4841.2

- e. Server hardening policy, which must cover all servers throughout the department, not only those that fall within the jurisdiction of the department's IT area. The policy must include the process for making changes based on newly published vulnerability information as it becomes available. Further, the policy must address, and be consistent with, the department's policy for making security upgrades and security patches.

Each state data center must carry out these responsibilities for those automated files and databases for which it has ownership responsibility. See SAM Sections 4841.4 and 4841.5.

Oversight responsibility at the agency level for ensuring the integrity and security of automated files and databases must be vested in the agency Information Security Officer.

The head of each agency is responsible for compliance with the policy described in this section. See SAM Section 4841.1.